IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

T.E., individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	
	)	Case No: 3:23-cv-303
v.	)	Division: Charlotte
AETNA INTERNATIONAL, LLC Serve Registered Agent: CT Corporation System 67 Burnside Ave. East Hartford, CT 06108	)	
and	)	
AETNA, INC. Serve Registered Agent: CT Corporation System 67 Burnside Ave. East Hartford, CT 06108	)	
and	)	
AETNA HEALTH MANAGEMENT, INC. Serve Registered Agent: CT Corporation System 67 Burnside Ave. East Hartford, CT 06108	)	
and	)	
AETNA HEALTH, INC. Serve Registered Agent: CT Corporation System 67 Burnside Ave. East Hartford, CT 06108	)	
and	)	
AETNA CORPORATE SERVICES, LLC	)	

Serve Registered Agent:
CT Corporation System
67 Burnside Ave.
East Hartford, CT 06108

and

AETNA RESOURCES, LLC
Serve Registered Agent:
CT Corporation System
67 Burnside Ave.
East Hartford, CT 06108

and

NATIONSBENEFITS, LLC,
Serve Registered Agent:
Caldera Law PLLC
7293 NW 2nd Avenue
Miami, FL 33150

and

NATIONSBENEFITS HOLDINGS, LLC,
Serve Registered Agent:
MWE Corporate Services, LLC
1007 North Orange Street
10th Floor
Wilmington, DE 19801

Defendants.

CLASS ACTION COMPLAINT FOR DAMAGES

COMES NOW ("Plaintiff"), individually and on behalf of all citizens who are similarly situated for her Class Action Complaint for Damages against Defendants Aetna International, LLC, Aetna, Inc., Aetna Health Management, Inc., Aetna Health, Inc., Aetna Corporate Services, LLC, and Aetna Resources, LLC (collectively hereinafter "Aetna") and NationsBenefits, LLC, and NationsBenefits Holdings, LLC (NationsBenefits, LLC and NationsBenefits Holdings, LLC

are sometimes referred to collectively as "NationsBenefits") (all Defendants are hereinafter sometimes referred to collectively as "Defendants") respectfully states and alleges as follows:

NATURE OF THE CASE

1. This is a class action brought by Plaintiff, individually and on behalf of all citizens who are similarly situated (*i.e.*, the Class Members), seeking to redress Defendants' willful and reckless violations of her privacy rights. Plaintiff and the other Class Members are customers of Defendant Aetna, a health insurance provider, who entrusted their Protected Health Information ("PHI") and Personally Identifiable Information ("PII") to Aetna. Defendant Aetna formed a Business Associate Agreement with Defendant NationsBenefits LLC and/or NationsBenefits Holdings LLC to provide its customers with life essential benefits with their health insurance company. As a part of the relationship between Aetna and NationsBenefits, Aetna has shared Plaintiff's PHI and PII with NationsBenefits who were entrusted to protect it and keep it from wrongful disclosure.

2. On or about January 30, 2023, an unauthorized third party or person accessed and downloaded Plaintiff's and the Class Members' PHI and PII. Defendants Aetna and NationsBenefits have independent, non-delegable duties to its customers to safeguard their PHI and PII and are responsible for the wrongful disclosure of Plaintiff's and the Class Members' PHI and PII.

3. This action pertains to Defendants unauthorized disclosure of the Plaintiff's PHI and PII that occurred between on or around January 30, 2023 (the "Breach").

4. Defendants disclosed Plaintiff's and the other Class Members' PHI and PII to unauthorized persons as a direct and/or proximate result of Defendants' failure to safeguard and protect their PHI and PII.

5. The wrongfully disclosed PHI and PII included, *inter alia*, Plaintiff's and the other Class Members' name, Social Security Number, physical address, date of birth, health plan subscriber numbers, Medicare Number, gender, and phone numbers.

6. Defendants flagrantly disregarded Plaintiff's and the other Class Members' privacy and property rights by intentionally, willfully, and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' PHI and PII from unauthorized disclosure. Plaintiff's and the other Class Members' PHI and PII was improperly handled, inadequately protected, readily able to be copied by anyone with nefarious intent and not kept in accordance with basic security protocols. Defendants' obtaining of the information and sharing of same also represent a flagrant disregard of Plaintiff's and the other Class Members' rights, both as to privacy and property.

7. Plaintiff and the other Class Members have standing to bring this action because as a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, Plaintiff and the other Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) identity theft, (iii) medical and pharmaceutical fraud, (iv) loss of medical expenses, and/or (v) the additional damages set forth in detail below, which are incorporated herein by reference.

8. Defendants' wrongful actions and/or inaction and the resulting Breach have also placed Plaintiff and the other Class Members at an imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud. Indeed, Javelin Strategy &

Research ("Javelin"), a leading provider of quantitative and qualitative research, released its 2012 Identity Fraud Report ("the Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PHI and PII is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiff's and the other Class Members' PHI and PII and not yet used the information will do so at a later date or re-sell it.

9. Plaintiff and the Class members have also suffered and are entitled to damages for the lost benefit of their bargain with Aetna Defendants and Defendants NationsBenefits. Plaintiff and members of the Classes paid Aetna and NationsBenefits for their services including the protection of their PHI and PII. The lost benefit of the bargain is measured by the difference between the value of what Plaintiff and the members of the Classes should have received when they paid for their services, and the value of what they actually did receive; services without adequate privacy safeguards. Plaintiff and members of the Classes have been harmed in that they (1) paid more for privacy and confidentiality than they otherwise would have, and (2) paid for privacy protections they did not receive. In that respect, Plaintiff and the members of the Classes have not received the benefit of the bargain and have suffered an ascertainable loss.

10. Additionally, because of Defendants' conduct, Plaintiff and members of the Classes have been harmed in that Defendants have breached their common law fiduciary duty of confidentiality owed to Plaintiff and member of the Classes.

11. Accordingly, Plaintiff and the other Classes seek redress against Defendants for breach of implied contract, outrageous conduct, common law negligence, invasion of privacy of public disclosure of private facts, negligent training and supervision, negligence *per se*, and breach of fiduciary duty of confidentiality.

12. Plaintiff, individually and on behalf of the other Classes, seeks all (i) actual damages, economic damages, and/or nominal damages, (ii) injunctive relief, and (iii) attorneys' fees, litigation expenses, and costs.

JURISDICTION AND VENUE

13. The Court has jurisdiction over the parties and the subject matter of this action. Jurisdiction is proper because Defendant Aetna is a business operating throughout the nation, including in North Carolina, whose principal place of business is in the state of Connecticut.

14. Jurisdiction is proper because Defendant NationsBenefits, LLC is a business organized in Florida and operating in the state of North Carolina whose principal place of business is at 1801 NW 66th Avenue, Suite 1000, Plantation, FL 33313. NationsBenefits, LLC is domiciled in Florida and is a citizen of Florida.

15. Jurisdiction is proper because Defendant NationsBenefits Holdings, LLC is a business organized in Delaware and operating in the state of North Carolina which is registered in the state of Delaware. NationsBenefits Holdings, LLC is a citizen of Delaware. Upon information and belief, the principal place of business of NationsBenefits Holdings, LLC is 1801 NW 66th Avenue, Suite 1000, Plantation, FL 33313.

16. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100

class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiff and members of the Class are citizens of states that differ from Defendants.

17. Venue is proper in the Western District of North Carolina, Charlotte Division, pursuant to 28 U.S. Code § 1391 because the acts complained of occurred, and Plaintiff is located, in the Western District of North Carolina, Charlotte Division.

PARTIES

18. Plaintiff is an adult residing in Mecklenburg County, North Carolina.

19. Aetna Defendants are, upon information and belief, nationwide companies with offices all throughout the country with their principal place of business at 151 Farmington Ave., Hartford, CT 06156. Aetna Defendants can be served at CT Corporation System, 67 Burnside Ave., East Hartford, CT 06108.

20. Defendant NationsBenefits, LLC is, upon information and belief, a nationwide company with offices throughout the country with its principal place of business at 1801 NW 66th Ave., Suite 100, Plantation, FL 33313. Defendant NationsBenefits, LLC may be served through its registered agent, to wit: Caldera Law, PLLC, 7293 NW 2nd Ave., Miami, FL 33150.

21. Defendant NationsBenefits Holdings, LLC is, upon information and belief, a nationwide company with offices throughout the country with its principal place of business at 1801 NW 66th Ave., Suite 100, Plantation, FL 33313. Defendant NationsBenefits Holdings, LLC's may be served through its registered agent, to wit: MWE Corporate Services, LLC, 1007 North Orange Street, 10th Floor, Wilmington, DE 19801.

BACKGROUND FACTS

22. Certain allegations are made upon information and belief.

23. Aetna Defendants are national health insurance companies pursuant to state and federal law, providing health insurance and medical services to the general public, operating at 151 Farmington Ave., Hartford, CT 06156.

24. Defendant NationsBenefits is a company which partners with Aetna to provide services and compensation for the life essential needs of its customers.

25. As a part of its business operations, Defendants collect and maintain PHI and PII of its customers.

26. Plaintiff and the Class Members are and/or were customers of Defendants and, as a result, provided their PHI and PII to Defendant.

27. Plaintiff and the Class Members entered into implied contracts with Defendants for the adequate protection of their PHI and PII.

28. Defendants are required to maintain the strictest privacy and confidentiality of Plaintiff and the proposed Classes' PHI and PII.

29. Aetna Defendants posts its privacy practices online, at https://www.aetna.com/legal-notices/privacy.html.

30. Defendant NationsBenefits posts its privacy practices online, at https://www.nationsbenefits.com/hipaa.

31. On or about April 27, 2023, Defendant NationsBenefits sent a letter to Plaintiff and the Class Members stating that a malicious actor(s) accessed or acquired the PHI and PII of customers of Aetna.

32. The letter from NationsBenefits stated that the personal information accessed or acquired by the malicious actor(s) included Plaintiff's and the Class Members' name, health plan subscriber number, gender, social security number, address, phone number and date of birth.

33. Recognizing the possibility of identity theft to the Plaintiff and the Class Members, both present and future, NationsBenefits offered two years credit monitoring through Experian Identityworks.

34. Defendants have made a substantial profit off of the unauthorized use and disclosure of Plaintiff's and the Class Members' PHI and PII.

35. The disclosure of the PHI and PII at issue was a result of the Defendants' inadequate safety and security protocols governing PHI and PII and its intent to profit off the use and disclosure of Plaintiff's and the Class Members' PHI and PII.

36. Upon information and belief, the Breach affected tens of thousands of Defendants' patients.

37. As a direct and/or proximate result of Defendants' failure to properly safeguard and protect the PHI and PII of its patients, Plaintiff's and the other Class Members' PHI and PII was stolen, compromised and wrongfully disseminated without authorization.

38. Defendants had a duty to their customers to protect them from wrongful disclosures.

39. As a business offering health insurance services, Defendants are required to train and supervise its employees and agents regarding the policies and procedures as well as the State and Federal laws for safeguarding patient information.

40. Aetna Defendants are covered entities pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendants must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

41. Defendant NationsBenefits is a business associate pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendant NationsBenefits must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

42. Aetna Defendants are covered entities pursuant to the Health Information Technology Act ("HITECH")[1]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

43. Defendant NationsBenefits is a business associate pursuant to the Health Information Technology Act ("HITECH")[2]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

44. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy in North Carolina. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

45. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

46. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. See 42 C.F.R. §§ 164.302-164.318.

47. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA

[1] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.
[2] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

48. HIPAA requires a covered entity or business associate to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

49. HIPAA requires a covered entity or business associate to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

50. Under HIPAA:

> Protected health information means individually identifiable health information:
>
> (1) Except as provided in paragraph (2) of this definition, that is:
>
> (i) Transmitted by electronic media;
>
> (ii) Maintained in electronic media; or
>
> (iii) Transmitted or maintained in any other form or medium.[3]

51. HIPAA and HITECH obligated Defendants to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that

[3] 45 C.F.R. § 160.103

had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

52. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

53. HIPAA further obligated Defendants to ensure that its workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

54. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[4] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represents the industry

[4] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[5]

55. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);
>
> (2) the recipient of the PHI;
>
> (3) whether the PHI was actually acquired or viewed; and
>
> (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[6]

56. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

57. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their roles in facility security.

[5] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
[6] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

58. Defendants failed to provide proper notice to Plaintiff and the Class Members of the disclosure.

59. Defendants failed to conduct, or improperly conducted, the four-factor risk assessment following the unauthorized disclosure.

60. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, the criminal(s) and/or their customers now have Plaintiff's and the other Class Members' compromised PHI and PII.

61. There is a robust international market for the purloined PHI and PII, specifically medical information. Defendants' wrongful actions and/or inaction and the resulting Breach have also placed Plaintiff and the other Classes at an imminent, immediate and continuing increased risk of identity theft, identity fraud[7] and medical fraud.

62. Identity theft occurs when someone uses an individual's PHI and PII, such as the person's name, Social Security number, or credit card number, without the individual's permission, to commit fraud or other crimes. *See* Federal Trade Commission, Fighting Back against Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/ about-identity-theft.html (last visited Jan. 18, 2013). The Federal Trade Commission estimates that the identities of as many as nine million Americans are stolen each year. *Id.*

63. The Federal Trade Commission correctly sets forth that "Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education,

[7] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia,* credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit." *Id.*

64. Identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (such as obtaining a driver's license or official identification card in the victim's name but with their picture), using a victim's name and Social Security number to obtain government benefits and/or filing a fraudulent tax return using a victim's information. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments and/or obtain medical services in a victim's name. Identity thieves also have been known to give a victim's PHI and PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

65. According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[8] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[9]

66. According to the Javelin Report, in 2011, the mean consumer cost of rectifying identity fraud was $354 while the mean resolution time of identity fraud was 12 hours. *Id.* at 6. In 2011, the consumer cost for new account fraud and existing non-card fraud increased 33% and 50% respectively. *Id.* at 9. Consumers who received a data breach notification had a fraud

[8] *Protecting Consumer Privacy in an Era of Rapid Change* FTC, Report March 2012 (http://www.ftc.gov/os/2012/03/120326privacyreport.pdf).

[9] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report*, 35-38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Comment of Center for Democracy & Technology,* cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12.

incidence rate of 19% in 2011 and, of those experiencing fraud, 43% reported their credit card numbers were stolen and 22% of the victims reported their debit card numbers were stolen. *Id.* at 10. More important, consumers who were notified that their PHI and PII had been breached were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification. *Id.* at 39.

67. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse. *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327 (http://www.ssa.gov/pubs/10064.html). Thus, a person whose PHI and/or PII has been stolen cannot obtain a new Social Security number until the damage has already been done.

68. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems; because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

69. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods. *See* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html. For example, as of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn, has led to a surge in

medical identity theft as a means of fraudulently obtaining medical care. "Victims of medical identity theft [also] may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits." *Id.*

70. Defendants flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiff's and the other Class Members' prior written consent to disclose their PHI and PII to any other person—as required by laws, regulations, industry standards and/or internal company standards.

71. Defendants flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiff's and the other Class Members' PHI and PII to unauthorized persons.

72. Upon information and belief, Defendants flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by failing to keep or maintain an accurate accounting of the PHI and PII wrongfully disclosed in the Breach.

73. Defendants flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and the other Class Members' PHI and PII to protect against anticipated threats to the security or integrity of such information. Defendants' unwillingness or inability to establish and maintain the proper information security procedures and controls is an

abuse of discretion and confirms its intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

74. The actual harm and adverse effects to Plaintiff and the other Class Members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendants' above wrongful actions and/or inaction and the resulting Breach requires Plaintiff and the other Class Members to take affirmative acts to recover their peace of mind, and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts—for which there is a financial and temporal cost. Plaintiff and the other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

75. Victims and potential victims of identity theft, identity fraud and/or medical fraud—such as Plaintiff and the other Class Members—typically spend hundreds of hours in personal time and hundreds of dollars in personal funds to resolve credit and other financial issues resulting from data breaches. *See Defend: Recover from Identity Theft*, http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/defend.html; *Fight Identity Theft*, www.fightidentitytheft.com. According to the Javelin Report, not only is there a substantially increased risk of identity theft and identity fraud for data breach victims, those who are further victimized by identity theft or identity fraud will incur an average fraud-related economic loss of $1,513 and incur an average of $354 of out-of-pocket expenses attempting to rectify the situation. *Id*. at 6.

76. Other statistical analyses are in accord. The GAO found that identity thieves use PHI and PII to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PHI and PII, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

77. Defendants' wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the other Class Members' PHI and PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Breach, Plaintiff and the other Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) identity theft, (iii) the imminent, immediate and continuing increased risk of identity theft, identity fraud and/or medical fraud, (iv) out-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance and/or other Breach risk mitigation products, (v) out-of-pocket expenses incurred to mitigate the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach, including the costs of placing a credit freeze and subsequently removing a credit freeze, (vi) the value of their time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Breach and (vii) the lost benefit of their bargain when they paid for their privacy to be protected and it was not.

CLASS ACTION ALLEGATIONS

78. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and the following proposed Nationwide Class and State Subclasses, defined as follows:

79. Plaintiff brings this class action as a class action on behalf of herself and the following classes:

> **All persons residing in the United States who were customers of Defendants Aetna and NationsBenefits since January 30, 2018 and whose PHI and/or PII was disclosed by Defendants to unauthorized third-parties.**
>
> **All persons residing in the United States who were residents of North Carolina who were patients of customers of Defendants Aetna and NationsBenefits since January 30, 2018 and whose PHI and/or PII was disclosed by Defendants to unauthorized third-parties (the "North Carolina Class").**

80. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

81. Plaintiff reserves the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

82. Numerosity: On information and belief, the putative Classes are comprised of tens of thousands of individuals, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

83. Commonality and Predominance: The rights of Plaintiff and each other Class Member were violated in a virtually identical manner as a direct and/or proximate result of Defendants' willful, reckless and/or negligent actions and/or inaction and the resulting Breach.

Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a) Whether Defendants willfully, recklessly and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the other Class Members' PHI and/or PII;

b) Whether Defendants were negligent in failing to properly safeguard and protect Plaintiff's and the other Class Members' PHI and/or PII;

c) Whether Defendants owed a duty to Plaintiff and the other Class Members to exercise reasonable care in safeguarding and protecting their PHI and/or PII;

d) Whether Defendants breached their duty to exercise reasonable care in failing to safeguard and protect Plaintiff's and the other Class Members' PHI and/or PII;

e) Whether Defendants were negligent in failing to safeguard and protect Plaintiff's and the other Class Members' PHI and/or PII;

f) Whether, by publicly disclosing Plaintiff's and the other Class Members' PHI and/or PII without authorization, Defendants invaded their privacy; and

g) Whether Plaintiff and the other Class Members sustained damages as a result of Defendants' failure to safeguard and protect their PHI and/or PII.

84. Adequacy: Plaintiff and her counsel will fairly and adequately represent the interests of the other Class Members. Plaintiff has no interests antagonistic to, or in conflict with, the other Class Members' interests. Plaintiff's lawyers are highly experienced in the prosecution of consumer class action and data breach cases.

85. Typicality: Plaintiff's claims are typical of the other Class Members' claims in that Plaintiff's claims and the other Class Members' claims all arise from Defendants' failure to properly safeguard and protect their PHI and PII.

86. Superiority and Manageability: A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff's and the other Class Members' claims. Plaintiff and the other Class Members have been harmed as a result of Defendants' wrongful actions and/or inaction and the resulting Breach. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct.

87. Class certification, therefore, is appropriate pursuant to Fed R. Civ. P. 23 because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

88. Policies Generally Applicable to the Case: Class certification also is appropriate pursuant to Fed. R. Civ. P. 23 because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

89. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights. Absent a class action, Defendants will retain the benefits of its wrongdoing despite its serious violations of the law.

90. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

91. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

92. Unless a Class-wide injunction is issued, Defendants may continue in its failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

COUNT I
BREACH OF IMPLIED CONTRACT

93. The preceding factual statements and allegations are incorporated herein by reference.

94. Plaintiff and the other Class Members, as part of their agreement with Defendants Aetna and NationsBenefits, provided Defendants their PHI and PII.

95. In providing such PHI and PII, Plaintiff and the other Class Members entered into an implied contract with Defendants, whereby Defendants became obligated to reasonably safeguard Plaintiff's and the other Class Members' PHI and PII.

96. Under the implied contract, Defendants were obligated to not only safeguard the PHI and PII, but also to provide Plaintiff and Class Members with prompt, adequate notice of any Data Breach or unauthorized access of said information.

97. Defendants breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their PHI and PII.

98. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the other Class Members' confidential medical information, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

99. Plaintiff and the other Class Members suffered and will continue to suffer

damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; and, (vii) emotional distress. At the very least, Plaintiff and Class members are entitled to nominal damages.

COUNT II
NEGLIGENCE
(On behalf of Plaintiff and the Class and the North Carolina Class)

100. The preceding factual statements and allegations are incorporated herein by reference.

101. Plaintiff brings this Count on her own behalf and on behalf of the Class and the North Carolina Class.

102. Defendants owed, and continues to owe, a duty to Plaintiff and the Classes to safeguard and protect their PHI and PII.

103. Defendants breached their duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiff's and the other Class Members' PHI and PII.

104. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PHI and PII would result in an unauthorized third-party gaining access to such information for no lawful purpose.

105. Plaintiff and the Classes entrusted their PII and PHI to Defendants on the premise and with the understanding that Defendants would safeguard their information, use

their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third-parties.

106. Defendants have full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Classes could and would suffer if the PII and PHI were wrongfully disclosed.

107. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Classes involved an unreasonable risk of harm to Plaintiff and the Classes, even if the harm occurred through the criminal acts of a third-party.

108. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII and PHI of Plaintiff and the Classes in Defendants' possession was adequately secured and protected.

109. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former patients', employees', and physicians' PII and PHI that Defendants was no longer required to retain pursuant to regulations.

110. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and the Classes.

111. Defendants' duty to use reasonable security measures arose as a result of the contractual relationship that existed between Defendants and Plaintiff and the Classes.

112. Defendants were also subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Classes.

113. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Classes was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

114. Plaintiff and the Classes were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting or redacting PII and PHI stored on Defendants' systems.

115. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and the Classes.

116. Defendants' misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions to not comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Classes, including basic encryption techniques freely available to Defendant.

117. Plaintiff and the Classes had no ability to protect their PII and PHI that was in, and possibly remains in, Defendants' possession.

118. Defendants were in a position to protect against the harm suffered by Plaintiff and the Classes as a result of the Data Breach. Defendants had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiff and the Classes within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and

the Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third-parties.

119. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Classes.

120. Defendants have admitted that the PII and PHI of Plaintiff and the Classes was wrongfully lost and disclosed to unauthorized third-persons as a result of the Data Breach.

121. Defendants, through their actions and/or omissions, unlawfully breached its duties to Plaintiff and the Classes by failing to implement industry standard protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Classes during the time the PII and PHI was within Defendants' possession or control.

122. Defendants improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Classes in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

123. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and the Classes in the face of increased risk of theft.

124. Defendants, through their actions and/or omissions, unlawfully breached its duty to Plaintiff and the Classes by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former patients', employees', and physicians' PII and PHI.

125. Defendants, through their actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Classes the existence and scope of the Data Breach.

126. As a direct result of Defendants' breach of their duty of confidentiality and privacy and the disclosure of Plaintiff's and the members of the Classes confidential medical information, Plaintiff and the members of the Classes suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation, and loss of enjoyment of life.

127. Plaintiff and the other Classes suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft and/or identify fraud; and, (vii) emotional distress. At the very least, Plaintiff and the other Classes are entitled to nominal damages.

128. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) negligence at common law. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

129. Defendants' conduct was particularly unreasonable given the nature and amount of PHI and PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Classes.

130. Defendants' violation of Section 5 of the FTC Act and Title II of HIPAA, including HIPAA regulations HHS has implemented pursuant to Title II, as well as the standards of conduct established by these statutes and regulations, constitutes negligence per se.

131. Plaintiff and the Classes are within the class of persons that the FTC Act was intended to protect.

132. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Classes.

133. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiff and the Classes have suffered and will suffer injury, including but not limited to:

a) actual identity theft;

b) the loss of the opportunity to control how their PII and PHI is used;

c) the compromise, publication, and/or theft of their PII and PHI;

d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI;

e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future

consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft;

f) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Classes; and

g) costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Classes.

135. As a direct and proximate result of Defendants' negligence and negligence per se, Plaintiff and the Classes have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

136. Additionally, as a direct and proximate result of Defendants' negligence and negligence per se, Plaintiff and the Classes have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

137. Plaintiff and the Classes are therefore entitled to damages, including actual and compensatory damages, restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

138. The preceding factual statements and allegations are incorporated herein by reference.

139. Plaintiff's and the other Classes' PHI and PII was (and continues to be) sensitive and personal private information.

140. By virtue of Defendants' failure to safeguard and protect Plaintiff's and the other Classes' PHI and PII and the resulting Breach, Defendants wrongfully disseminated Plaintiff's and the other Class Members' PHI and PII to unauthorized persons.

141. Dissemination of Plaintiff's and the other Classes' PHI and PII is not of a legitimate public concern; publicity of their PHI and PII was, is and will continue to be offensive to Plaintiff, the other Class Members and all reasonable people. The unlawful disclosure of same violates public mores.

142. As a direct result of Defendants' breach of their duty of confidentiality and privacy and the disclosure of Plaintiff's and the members of the Classes' confidential medical information, Plaintiff and the members of the Classes suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation, and loss of enjoyment of life.

143. Plaintiff and the other Classes' members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft and/or identify fruad; and, (vii) emotional distress. At the very least, Plaintiff and the other Classes' Members are entitled to nominal damages.

144. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and the other Classes' Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT IV
BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY

145. The preceding factual statements and allegations are incorporated herein by reference.

146. At all times relevant hereto, Defendants owed, and owes, a fiduciary duty to Plaintiff and the proposed class pursuant to North Carolina common law, to keep Plaintiff's medical and other PHI and PII information confidential.

147. The fiduciary duty of privacy imposed by North Carolina law is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530 which requires a covered entity or business associate to apply appropriate

administrative, technical, and physical safeguards to protect the privacy of patient medical records.

148. Defendants breached their fiduciary duty to Plaintiff by disclosing Plaintiff's and the other Classes' Members' PHI and PII to unauthorized third-parties.

149. As a direct result of Defendants' breach of fiduciary duty of confidentiality and the disclosure of Plaintiff's confidential medical information, Plaintiff and the proposed Classes' Members suffered damages.

150. As a direct result of Defendants' breach of their duty of confidentiality and privacy and the disclosure of Plaintiff's and the members of the Classes' confidential medical information, Plaintiff and the members of the Classes suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

151. Plaintiff and the other Classes' Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft and/or fraud; and, (vii) emotional distress. At the very least, Plaintiff and the other Classes' Members are entitled to nominal damages.

COUNT V
NEGLIGENT TRAINING AND SUPERVISION

152. The preceding factual statements and allegations are incorporated herein by reference.

153. At all times relevant hereto, Defendants owed and owe a duty to Plaintiff and the Classes to hire competent employees and agents, and to train and supervise them to ensure they recognize the duties owed to their patients and their parents.

154. Defendants breached their duty to Plaintiff and the member of the Classes by allowing its employees and agents to give access to patient medical records to an unauthorized user.

155. As a direct result of Defendants' breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and the members' of the Classes confidential medical information, Plaintiff and the members of the Classes suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

156. Plaintiff and the other Classes' members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft and/or identify fraud; and, (vii) emotional distress. At the very least, Plaintiff and the other Classes' Members are entitled to nominal damages.

157. Defendants' wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and the other Classes' Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PHI and PII) without their authorization or consent.

COUNT VI
NEGLIGENCE *PER SE*

158. Plaintiff incorporates by reference and re-alleges all paragraphs previously alleged herein.

159. Plaintiff was under the medical care of the Defendant.

160. Defendant Aetna is a covered entity for purposes of HIPAA and HITECH.

161. Defendant NationsBenefits is a business associate for the purposes of HIPAA and HITECH.

162. Plaintiff is a member of the class HIPAA and HITECH were created to protect.

163. Plaintiff's private health information is the type of information HIPAA and HITECH were created to protect. HIPAA and HITECH were created to protect against the wrongful and unauthorized disclosure of an individual's health information.

164. Defendants gave protected medical information to an unauthorized third-party or unauthorized third-parties without the written consent or authorization of Plaintiff.

165. Defendants gave protected medical information to unauthorized third-parties without Plaintiff's oral consent or written authorization.

166. The information disclosed to an unauthorized third-party or unauthorized third-parties included private health information about medical treatment.

167. Alternatively, Defendants violated HIPAA and HITECH in that they did not reasonably safeguard the private health information of Plaintiff from any intentional or

unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements pursuant to HIPAA and HITECH including, but not limited to, 42 C.F.R. §§ 164.302-164.318, 45 C.F.R. § 164.500, *et seq*, and 42 U.S.C. §17902, and was therefore negligent *per se*.

168. As a direct result of Defendants' negligence, Plaintiff and the Classes suffered damages and injuries, including, without limitation, loss of the benefit of their bargain, a reduction in value of their private health information, loss of privacy, loss of medical expenses, loss of trust, loss of confidentiality, embarrassment, humiliation, emotional distress, and loss of enjoyment of life.

169. Plaintiff and the other Classes suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of their PHI and PII; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft and/or identify fraud; and, (vii) emotional distress. At the very least, Plaintiff and the other Classes are entitled to nominal damages.

170. As a direct result of Defendants' negligence, Plaintiff and the Classes have a significantly increased risk of being future victims of identity theft relative to what would be the case in the absence of the Defendants' wrongful acts.

171. As a direct result of Defendants' negligence, future monitoring, in the form of identity-theft or related identity protection is necessary in order to properly warn Plaintiff and the Classes of, and/or protect Plaintiff and the Classes from, being a victim of identity theft or other

identity-related crimes. Plaintiff, individually and on behalf of the Classes, seeks actual damages for all monies paid to Defendants in violation of the HIPAA and HITECH. In addition, Plaintiff seeks attorneys' fees.

COUNT VII
INVASION OF PRIVACY

172. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein. Plaintiff brings this Count on her behalf and on behalf of the Classes.

173. Plaintiff and the Classes had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

174. Defendants owed a duty to their current and former customers including Plaintiff and the Classes, to keep their Private Information contained as a part thereof, confidential.

175. Defendants failed to protect, and released to unknown and unauthorized third parties, the PII and PHI of Plaintiff and the Classes.

176. Defendants allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiff and the Class, by way of Defendants' failure to protect the PII and PHI.

177. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and the Classes is highly offensive to a reasonable person.

178. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Classes disclosed their Private Information to Defendants as part of

their medical care or employment with Defendants, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Classes were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

179. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiff's and the Classes' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

180. Defendants acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

181. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Classes.

182. As a proximate result of the above acts and omissions of Defendants, the Private Information of Plaintiff and the Classes was disclosed to third parties without authorization, causing Plaintiff and the Classes to suffer damages.

Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Classes in that the PII and PHI maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Classes have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Defendants, as follows:

A. Declaring that this action is a proper class action, certifying the Classes as requested herein, designating Plaintiff as Class Representative and appointing Plaintiff's counsel as Lead Counsel for the Classes;

B. Declaring that Defendants' conduct was extreme and outrageous;

C. Declaring that Defendants breached their implied contract with Plaintiff and Classes;

D. Declaring that Defendants negligently disclosed Plaintiff's and the Classes' Members' PHI and PII;

E. Declaring that Defendants have invaded Plaintiff's and Classes' Members' privacy;

F. Declaring that Defendants breached their fiduciary duty to Plaintiff and the Classes;

G. Declaring that Defendants breached their implied contract with Plaintiff and the Classes;

H. Declaring that Defendants were negligent by negligently training and supervising its employees and agents;

I. Ordering Defendants to pay actual damages to Plaintiff and the Classes;

J. Ordering Defendants to properly disseminate individualized notice of the Breach to all Classes;

K. For an Order enjoining Defendants from continuing to engage in the unlawful business practices alleged herein;

L. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiff and the Classes;

M. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

N. Ordering such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial.

This 20th day of May, 2023.

Respectfully submitted,

/s/Emily J. Beeson
Emily J. Beeson
NC State Bar No. 47567
Ward Black Law
208 W. Wendover Ave.
Greensboro, NC 27407
Ph: 336-333-2244
Fax: 336-510-2163
ebeeson@wardblacklaw.com

/s/ Maureen M. Brady
Maureen M. Brady KS #22460
Lucy McShane KS #22517
(*pro hac vice* petition forthcoming)
McShane & Brady, LLC
1656 Washington Street, Suite 120
Kansas City, MO 64108
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
E-mail: mbrady@mcshanebradylaw.com
lmcshane@mcshanebradylaw.com

/s/Sharon J. Zinns
Sharon J. Zinns, Esq.
(pro hac vice petition forthcoming)
Georgia Bar No. 552920
ZINNS LAW, LLC
4243 Dunwoody Club Drive
Suite 104
Atlanta, GA 30350
Tel: (404) 882-9002
Email: sharon@zinnslaw.com

/s/John A. Love
John A. Love
(*pro hac vice* petition forthcoming)
GA Bar No. 459155
LOVE CONSUMER LAW
2500 Northwinds Parkway
Suite 330
Alpharetta, GA 30009
tel: 404.855.3600
fax: 404.301.2300
Email: tlove@loveconsumerlaw.com